Q-4394
Ref.
OLC #78-3053
Rec'd 21 Aug 78

D R A F T

REPORT OF

THE

SELECT COMMITTEE ON INTELLIGENCE

SUBCOMMITTEE ON SECRECY AND DISCLOSURE

NATIONAL SECURITY SECRETS: THEIR PROPER PLACE IN THE LAW

Helen - pls. have registry file one copy of the draft report - the others can be destroyed. It should be indicated that the draft was the subject of Lapham's letter of 26 Sept.

August 11, 1978

TABLE OF CONTENTS

I. PREFACE

> The President learned of the new horror. Bletchley (the site in England where British intelligence was decoding German military communications) was discovering ahead of time which civilian targets Hitler planned to strike next. Churchill and his War Cabinet had to decide which was more important: to warn the families marked for punishment or protect the secrets of Bletchley's growing apparatus for divining Nazi intentions.
> A Man Called Intrepid by William Stevenson.

The secrecy necessary for effective intelligence activities often forces upon government officials difficult moral dilemmas. A Man Called Intrepid is the story of the secret extralegal British and American intelligence apparatus established by Churchill and Roosevelt to combat the German war machine. The book is rife with anecdotes about difficult decisions by the President and the Prime Minister involving the need to protect the ULTRA secret (the fact that the allies had cracked the German code). Certainly the most famous of these was the foreknowledge allegedly provided Churchill through ULTRA of the German plans to firebomb Coventry.

According to Stevenson, Churchill decided not to evacuate Coventry out of fear that the Germans would realize the British had broken their code.* When confronted with Churchill's decision on Coventry and similar questions, Roosevelt is said to have remarked, "War is forcing us more and more to play God."

---

* Critics of Stevenson's book contend that this anecdote is inaccurate. Nonetheless, there is little doubt that Churchill had to face many agonizing decisions in which he decided not to forewarn citizens for fear of jeopardizing the ULTRA secret.

Since World War II, intelligence activities and concomitant secrecy have increased rather than subsided. The moral dilemmas have increased. Certainly most officials of British and American intelligence would agree with Sir William Stephenson, the man code-named "Intrepid":

> We live in a world of undeclared hostilities in which such weapons (the weapons of secrecy) are constantly used against us and could, unless countered, leave us unprepared again, this time for an onslaught of magnitude that staggers the imagination.

Stephenson concludes his discussion of the need for secrecy with the following insight:

> So there is the conundrum: how can we wield the weapons of secrecy without damage to ourselves? How can we preserve secrecy without endangering constitutional law and individual guarantees of freedom?

Stephenson expresses the conventional concern that secrecy could undermine democratic principles, and no one who has lived through the past few years can deny the price that we have sometimes paid for secrecy in intelligence and government. However, in the course of our study of secrecy we found that there is a part of the present-day dilemma which Stephenson does not mention. Indeed it is not unlike the problem of foreknowledge faced by Churchill and Roosevelt in "Coventry-type" situations. Secrecy and a desire on the part of the intelligence community to preserve secrets has at times, posed certain threats to the national security itself. This report demonstrates the fact that the more sensitive the information compromised, the more difficult it becomes to enforce the laws that guard our national secrets. This occurs principally because the legal

steps necessary to pursue a breach entail, almost inevitably, some further compromise of sensitive material. This is not a problem which is likely to be corrected by a revision of our substantive espionage statutes.

This impasse may not only adversely affect national security but also threatens the administration of justice. Intelligence agencies through the last several decades have, in the name of "protecting sources and methods", attempted to hold themselves apart from the rest of the Executive branch and the Congress. This phenomenon fostered the belief among some intelligence officials that they were subject to a different standard of law. Certainly secrecy and that estrangement were important causes of recent crises concerning the intelligence agencies.

no inkling of change — debunk & suggest this is true today. Very offensive.

Therefore, the real dimensions of the problem that the staff has discovered are broader than the conundrum posed by Stephenson. The basic dilemma facing the intelligence community, the Executive branch and this Committee is not just whether secrecy and democracy are compatible, but whether maintaining secrecy at any cost can undermine the national security, the enforcement of the espionage statutes, and the general administration of justice. In the words of one Justice Department official who testified before the Subcommittee, "To what extent must we harm the national security in order to protect the national security?"

ILLEGIB

[redacted] statement of issue — can only be one answer obscures prob not illuminates

Joseph R. Biden, Jr., Chairman
James Pearson, Vice Chairman
Subcommittee on Secrecy
and Disclosure

II. SUMMARY

The Committee's inquiry has led it to the following conclusions:

(A) There is a major breakdown in the administration of the criminal espionage statutes in leak cases. To date, we have been unable to identify a single successful prosecution of an individual who leaked classified information to a publication. This record was found despite the nearly unanimous assessment that at least some leaks violate existing statutes and cause serious harm to our national security.

The breakdown results in part from an impasse between the Department of Justice and the intelligence community on how to deal with the further use of classified information necessary for investigation and prosecution of these cases. Briefly stated, there is no formal mechanism to weigh the risks of additional disclosures against the benefits of prosecution.

(B) Congressional efforts to remedy this breakdown should first be directed at improving the administration of current statutes; Congress should defer consideration of new criminal sanctions until enforcement problems are eliminated or substantially reduced.

(C) Disagreements over the use of classified information also impede classical espionage prosecutions.

(1) The Committee reviewed some classical espionage cases which have not proceeded to either investigation or prosecution for the same reason that leak cases cannot

proceed -- concern about the disclosure of intelligence information in the course of investigation or prosecution. Furthermore, certain cases engendered such intense disagreements between the intelligence community and the Department of Justice that Presidential intervention to resolve the disagreement was almost required.

(2) However, a resolution of the disagreement over the use of classified information in espionage prosecutions is likely for the following reasons:

(a) Classical espionage cases are generally considered more serious than leak cases.

(b) The federal espionage statutes are more clearly drawn to cover classical espionage than most leaks.

(c) Many classical espionage cases are in effect out of the control of the intelligence community because the law enforcement machinery has been engaged by an arrest, or because the public or officials outside the intelligence community know of the crime and, therefore, pressure the intelligence community to provide information necessary for prosecution.

(d) Usually the constitutional problems (primarily First Amendment problems) are much less severe in classical espionage cases than in leak cases.

(D) The impasse over the use of classified information occurs in other types of criminal cases and at times defendants

may have placed the Department of Justice at a marked disadvantage because of this dilemma in perjury, narcotics, and even murder cases.

The Committee has formulated a series of recommendations designed to alleviate the problems faced by the government in maintaining the secrecy of legitimate national security information. These recommendations can be found on pages

III. BACKGROUND OF SECRECY AND DISCLOSURE SUBCOMMITTEE INQUIRY

On April 26, 1977, the Subcommittee asked the staff to undertake (1) a review of unauthorized disclosures of intelligence information and (2) an inquiry into the use of compartmentation -- a procedure to place special limitations on access to information that is especially sensitive. Although some progress has been made on the second inquiry, most of the Subcommittee's work has concentrated on the first question which will serve as the focus of this report.

The Subcommittee conducted its inquiry through both interviews and file searches at the intelligence agencies. We have conducted over thirty interviews and briefings with officials of the Departments of Justice and State and the major intelligence agencies (CIA, NSA and DIA). In the course of these briefings we asked each agency to provide us with ten cases in which intelligence information had been covertly passed to foreign powers -- classical espionage cases -- or in which intelligence found its way into the public media -- intentional or accidental leak cases. We have reviewed over forty case files or summaries of case files provided by these agencies. These files have served as a valuable data base for our survey. Indeed, we believe that they represent the most comprehensive compilation of such information in either the Executive branch or Congress. Each file contains information on an intelligence compromise which has occurred in the last few years, the action taken -- or not taken, as is frequently the case -- by the

relevant agency or the FBI, and any disciplinary action taken against the individuals responsible.

In June of last year, after reviewing a summary of the results of its survey, and based on a number of surprising findings, the Subcommittee redirected its inquiry. The Subcommittee began on the assumption that the major issue to be addressed would be evaluating the desirability of additional criminal sanctions for unauthorized disclosure of information that jeopardized sensitive foreign intelligence "sources and methods". However, as the work proceeded, the Subcommittee was soon driven to the conclusion that no present statute can be effectively enforced against "leaks" and that it would be a difficult task to draft a constitutional criminal statute which would solve the enforcement problems. In fact, the nation's strictest statutory safeguard against unauthorized disclosure, Section 798 of Title 18, the U.S. espionage statute which protects communications intelligence "sources and methods" in a manner similar to that of the British Official Secrets Act, does little to deter either classical espionage or leaks. The files which the Subcommittee has studied reveal several cases in which violations of even this statute were neither investigated nor prosecuted.

At the heart of this failure of enforcement is a very deep-seated conflict between the interests of the intelligence community on the one hand, and the Department of Justice on the other over the enforcement of the espionage statutes. The conflict arises over whether the intelligence community and Defense Department, which are charged with protecting the

national security, or the Department of Justice, which is charged with enforcing the law, should prevail in controlling the use of classified information necessary to conduct the investigation and to proceed with the prosecution.* Indeed this question of whether or which classified information is to be used in a particular judicial proceeding is a pervasive problem that goes well beyond enforcement of the espionage statutes. Problems created by classified information have also hampered many other prosecutions, including perjury, extortion, bribery, narcotics violations and possibly even one murder case.

On March 1st, 2nd and 6th, the Subcommittee on Secrecy and Disclosure conducted public hearings on the matters raised by our inquiry. The Subcommittee heard from Admiral Stansfield Turner, the Director of Central Intelligence; Benjamin Civiletti, the Acting Deputy Attorney General; Philip Lacovara, formerly of the Watergate Special Prosecutor's Office; Judge Fletcher, Chief Judge of the Court of Military Appeals; William Colby, former Director of Central Intelligence; Lawrence Houston, former CIA General Counsel; and Morton Halperin, representing the American Civil Liberties Union. The purpose of this report is to summarize the Committee's findings based on these hearings and its year-long inquiry, and to report its recommendations for

---

* It is common knowledge that the FBI and other counter-intelligence agencies do from time to time decide not to prosecute espionage cases for other reasons such as the desirability of monitoring a particular spy in order to understand the full dimensions of a spy network. This report does not address these kinds of cases but only those where investigation and prosecution is the preferred approach.

legislative and administrative actions to facilitate administration of certain statutes related to the national security.

IV. "LEAK" AND CLASSICAL ESPIONAGE INVESTIGATIONS

A. "Leak" Investigations

The Subcommittee examined thirty recent cases submitted by the CIA, NSA and DIA. These cases consisted primarily of instances of leaks of intelligence information to the newspapers. Of those thirty cases only three were actually referred to the Department of Justice for investigation and none of those was formally investigated. All were recent cases. Almost half of the cases involved disclosure of communications intelligence, which could have been prosecuted under Section 798 of Title 18 of the United States Code (see Appendix). As noted earlier, Section 798 is the only espionage provision presently on the books that approaches the strict liability criminal standard used by the British in the Official Secrets Act, the model for recent proposals to create new criminal sanctions for "leaks".

Many of these "leak" cases are not investigated by the FBI because the Department of Justice has developed a policy of refusing to investigate unless the intelligence community is willing to declassify all information related to the case. This policy grew out of frustration by the Department over the years with intelligence community reluctance to provide necessary evidence to prosecute major leak cases after the FBI had invested considerable time and effort in investigation.

The response to those leaks which are subject to internal intelligence agency investigations, such as they are, begins with an employee of an intelligence agency who is familiar with the intelligence and who identifies the possible leak when it is published. In other words, if the intelligence relates to

information gleaned from communications intelligence, an employee of the unit which processes that intelligence would probably recognize the sensitivity of the published information and report it to the office of security of his agency. The office of security then would notify the office of public affairs. Upon receipt of the published article containing the leak, the office of security of the concerned intelligence agency would next attempt to determine the individuals or offices who had access to the information.

This type of investigation is often fruitless because the leaked information has been disseminated broadly in such inter-agency classified materials as certain CIA intelligence cables, the National Intelligence Daily or the Weapons Intelligence Summary (some of which have circulation in the thousands). The very information which must be disseminated to policymakers is frequently the information which requires the greatest protection from unauthorized disclosure. At the same time that the security office is attempting to determine the scope of dissemination and the possible recipients of the information, it is working closely with the office within the intelligence agency where the information originated in the preparation of a damage assessment.*

---

* Most of the damage assessments that were reviewed were quite perfunctory in nature and provide no specific information on the actual and specific damage caused by the leak.

In fairness to those preparing the damage assessment at such an early date in the process, it is difficult to assess the damage because it is not yet clear whether or not a hostile power has actually responded to the information in the article. However, damage assessments were rarely updated in the cases which were reviewed.

After the damage assessment is completed and a cursory review of the number of people who might have had access is finished, the information is forwarded to one of three organizations: to the Security Committee of the Intelligence Community Staff, to another agency if it is clear that the information must have been leaked by a publication or office or individuals of that agency, or (in a small fraction of the cases) to the Department of Justice.

If reference to the Department of Justice is indicated, the Department's response is pro forma. The Department of Justice does not usually initiate an investigation. It normally responds with a letter back to the agency containing what is called "the eleven questions" (see Appendix). Neither the Department of Justice nor the FBI will normally proceed further until the eleven questions are answered. Some of the eleven questions are uncontroversial -- such as whether the compromised information was properly classified in the first place and whether the article disclosing it was accurate. In most cases, particularly those of extreme sensitivity, however, the whole process reaches an impasse at Question 9, which reads as follows:

> Whether the data can be declassified for the purpose of prosecution and, if so, the name of the person competent to testify concerning the declassification.

The intelligence agencies view this as a requirement that they agree to declassify any and all information in question before the Department of Justice will agree to investigate the case. Since the agencies rarely agree to this "up front" commitment, few cases, if any, are ever actually investigated by

the Department of Justice. Indeed, of the 30 cases provided by the intelligence agencies, none was investigated by the Department of Justice.

B. Classical Espionage Investigations

Classical espionage cases -- secretly passing classified information to a hostile power -- are taken much more seriously than leaks by both the Justice Department and the intelligence community. (See discussion on page) Despite the fact that classical espionage cases and "leaks" may both be prosecuted under the same criminal statutes, the eleven question leak questionnaire is not used in espionage cases. Indeed in classical espionage cases a resolution is almost always reached between the intelligence community and the Justice Department on how to proceed with investigation. Although the government is capable of resolving its differences in classical espionage cases, the decision is often made not to prosecute. Therefore the initial impasse that prevents the opening of investigations in leak cases does not occur. Nevertheless, even if the decision is to proceed to trial, it is often a painful and hotly contested matter causing friction between the Justice Department and the intelligence community from the grand jury proceedings through sentencing. The Subcommittee examined cases that did proceed to prosecution and one case which was subsequently dropped with no punitive action taken against an individual who admitted to espionage.

e.g. C. Song — can't be supported — STAT — only — several espionage cases in the past 2½ years

United States v. Moore was the successful prosecution last year of a former CIA official who tossed classified documents

onto the Russian Embassy lawn here in Washington. United States v. Boyce and Lee, also successfully prosecuted last year, involves an employee of TRW, a large defense contractor in California, who passed photographs of documents describing extremely sensitive intelligence systems to the Russians. Both cases were the subject of considerable tension between the CIA and the Department of Justice. Both required protracted negotiations on whether to use individual documents and witnesses in the trial. In one case friction over those sorts of issues became so intense that the lawyer assigned responsibility in CIA's Office of General Counsel refused to participate any further. In the Moore case disagreements between DCI George Bush and Attorney General Levi almost required President Ford's intervention on his last day in office.

C. Damage by Confirmation Versus Augmentation

The intelligence agencies' concern about the effect of investigation or prosecution of a leak or classical espionage upon the national security falls into two basic categories:

(1) The investigation or prosecution of an espionage violation can further damage the national security by confirming the validity of the information disclosed. For example, in either a covert transmission case or a leak case a hostile power which discovers information very sensitive to the national security may discount the information because of questions about the reliability of the source, whether it be a spy or a newspaper. However, if an indictment is filed against the subject or the existence of an investigation is disclosed, the

hostile intelligence service tends to interpret that indictment or investigation as confirmation of the accuracy of the information provided. This particular form of damage to the national security is practically impossible to remedy because of the constitutional requirement of a "public" trial -- the defendant has a right to a public adjudication of the charges against him. This is one reason why criminal sanctions for even the most serious "leaks" to newspapers would be a particularly counter-productive remedy.

(2) Investigation or prosecution may augment the damage to the national security by disclosing either to the defendant or other interested parties further information necessary either to investigate the case or to prove the case. For example, it frequently becomes necessary in the course of investigation to discuss the facts of the case with a variety of witnesses who may be associates of the defendant. In a criminal case there is a plethora of procedures which involve public discussion of evidence related to the crime. This may be particularly risky in espionage cases where prosecution may disclose sophisticated counter-espionage techniques.

D. Augmentation of the Damage in Criminal Cases

This latter problem, augmentation of the damage, may be easier to resolve than the former. Where the Justice Department has determined to proceed, for example as in the Rosenberg or Ellsberg case, or in the two major espionage prosecutions last year, the prosecutors and judges have fashioned ad hoc procedures to protect the national security and at the same time ensure the

administration of justice. These ad hoc procedures form the focus of the Committee's present efforts.

In a criminal prosecution involving perjury, narcotics smuggling, organized crime offenses such as extortion, or espionage, there are a variety of circumstances in the course of pre-trial or trial procedures in which government attorneys fear a judge will require disclosure of classified information.

(1) As part of the case against the defendant. In a typical espionage prosecution, classified information may be directly relevant in proving the case against the defendant. For example, in a prosecution under Section 793 of Title 18, it is necessary to prove that the information passed will actually damage the national security or be of aid to a foreign government. Of course, in some cases the information passed is not of obvious significance to a foreign government and there is always the likelihood the foreign government does not understand the impact of the information passed. In such a criminal trial it becomes necessary to explain to the jury, and therefore to the public, the significance of the information passed. For example, in the Moore case the government had to publicly disclose the names of individuals in the CIA telephone directory (among the documents tossed onto the Embassy lawn, but which in fact was never examined by the Russians).*

poor discussion of Moore

---

*, In this case the Federal judge took the extraordinary step of sealing a public trial exhibit (consisting of the directory and other sensitive documents), permitting only limited access by the jury and the public. not to jury - public only

The Boyce and Lee prosecution earlier this year was one of the very few prosecutions under Section 798 of Title 18 for the unauthorized dissemination of communications intelligence. However, even though that statute does not require proof of harm, it was necessary to prove that the information was appropriately classified and in the course of such a procedure it was necessary to offer evidence that indicates the significance of the information passed.

(2) As a part of the defendant's affirmative defense. In the course of any of these prosecutions it is likely that the defendant may successfully raise an affirmative defense that will require classified information. For example, an agency official prosecuted for deceiving Congress, might offer the affirmative defense that it was a pattern or practice of Agency officials either to conceal classified information in Congressional briefings or even to deceive Congressional committees. In the alternative, the official might argue that the information he provided the Committee was indeed truthful. Obviously both of these offers of proof would have required the disclosure of a considerable amount of extremely sensitive, classified information. In cases of organized crime and narcotics smuggling, a defendant might raise his former association with the Agency as part of a putative affirmative defense which would require evidence of the CIA's relationship to him or similar agency relationships to other individuals in the underworld.

ILLEGIB

(3) As part of pre-trial discovery. In every criminal trial the defendant is entitled under the Constitution,

under statute, or under the Federal Rules of Criminal Procedure*, to: (a) all materials obtained from or belonging to the defendant; (b) information pertaining to the testimony of a government witness; and, (c) any exculpatory information within the government's possession. Frequently the information which must be disclosed in these pre-trail procedures is classified.

see 16

E. "Gray Mail": The Price of Failing To Resolve The Dilemma

Since the Espionage Act was enacted in 1917, the Federal Government has been cautious in using the statute because of the necessity to provide further classified information in the course of a prosecution. Prosecutors in the Department of Justice and intelligence community officials have always recognized that the espionage statute is not an effective remedy for all "leaks" to the newspaper or covert transmission to a foreign spy because of the counter-productive disclosure of further secrets. The Department of Justice is also aware that a defense counsel, in the course of trial or through pre-trial discovery, can threaten the government with frivolous discovery motions or a line of questioning that discloses or requires the disclosure of classified information. An internal CIA study of this problem in 1966 characterizes the dilemma as follows:

---

* See Rule 16, F.R. Crim. P.

> Out of this evidentiary difficulty has come a sort of "gray mail", granted on the immunity from prosecution (and often civil suit as well) enjoyed by the thief who limits his trade to information too sensitive to be revealed.

So long as the defendant threatens to reveal sensitive information in the course of a trial, he or she may engage in this "gray mail" which precludes prosecution.

Disagrees with this conclusion

V. "TO KILL...TO LIE, CHEAT AND SPY"

terribly offensive

> ...Agent 007, had a license to kill, but I think the testimony and the findings of the Subcommittee staff...support the judgment that the situation in real life is even more sweeping than Ian Fleming wrote of in his fictional novels...People... connected with intelligence information, whether they are themselves intelligence officers or otherwise involved with national security operations, have by virtue of the immunity from prosecution something like a license not only to kill, but to lie, steal, cheat, and spy...

STAT [redacted] in testimony before the Subcommittee on Secrecy and Disclosure.

The ambiguity of the statutes described in previous sections and the internal Executive branch procedures for their enforcement have created a legal vacuum -- tantamount to immunity -- for people who gain access to secret information. The dilemma is most often confronted in the leak and classic espionage circumstances described earlier, but occurs as well in cases not usually associated with the national security -- bribery, extortion, obstruction of justice or murder.*

The following are actual cases in the public record where secrecy and concerns about disclosure of sources and methods actually interfered with the investigation or prosecution of a serious felony which was not directly related to the national security. These cases are important not only because they represent the different kinds of crimes which give rise to this phenomena but also the subtlety with which concern

worst taste of [illegible] I know what to do with it

* There are no examples of leaks or classical espionage cases halted for national security reasons included below because any further public discussion of these cases might raise the same concerns as investigations or prosecutions -- further disclosure of legitimate national secrets.

about sources and methods can interfere with the administration of justice.

A. A Case of Bribery

In his book The American Black Chamber published in 1933, Herbert Yardley, who directed the United States' first signals intelligence operation, describes an incident concerning a message which he intercepted between a foreign Ambassador in Washington and his home government. The message implicated the Ambassador in bribery of a high American government official and his secretary.

In a subsequent meeting with a high official in the State Department, Yardley admitted having sent the message to the Attorney General. The State Department official and the Secretary were furious that the Attorney General knew the contents of the intercept even though it pertained to serious criminal activity by government officials.

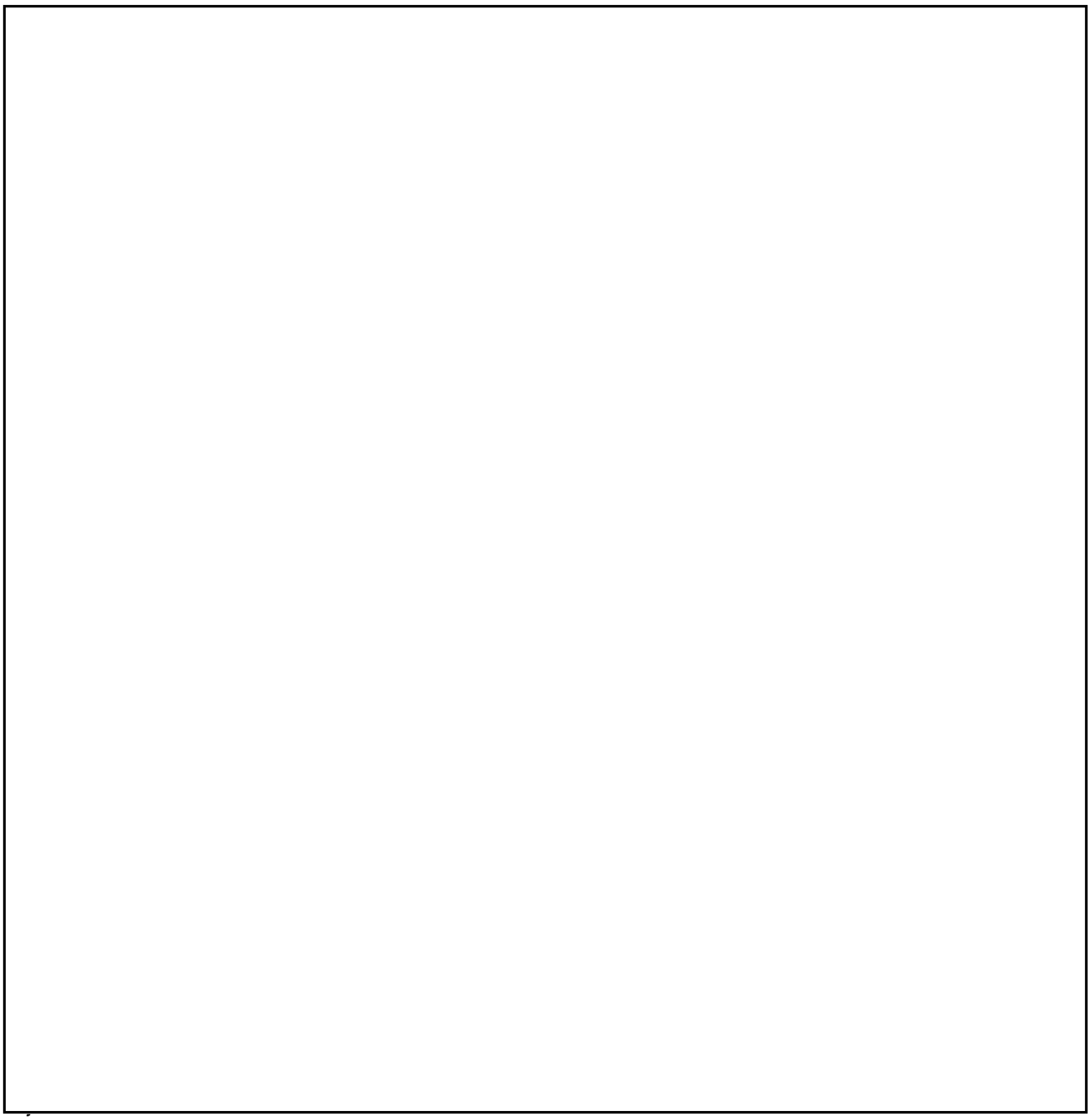
Yardley had thought it appropriate to send this message over because it looked to him like a Justice Department case. The State Department official was adamant. "The activity of an Ambassador is never a Justice Department case," he stated.

Yardley himself warned that if the Ambassador were recalled, "His government will appoint a new ambassador, install a new code, and one never knows how much difficulty a new code will cause." Yardley continued:

> The new Ambassador will probably engage in the same sort of activities, but we may not be in a position to know just what is going on. Isn't it more desirable to keep this Ambassador here and know what he is up to than to have a new one without being certain that we can check up on his activities?

The State Department official responded:

Yes we have thought of all that. My impression is the entire case will be dropped. It is too serious to meddle with.*



STAT

* Yardley, Herbert, The American Black Chamber (1933).

Next 7 Page(s) In Document Exempt

Approved For Release 2004/04/13 : CIA-RDP81M00980R002800010045-2

VI. PAST LEGISLATIVE AND ADMINISTRATIVE PROPOSALS IN RESPONSE TO THE "GRAY MAIL" PHENOMENA

Over the years the CIA and its predecessors have responded with two initiatives to the problems of enforcement of the espionage and other statutes which risk disclosures of foreign intelligence "sources and methods". First, especially with respect to leaks and espionage violations, military and intelligence agencies have called for enactment of statutes similar to the British Official Secrets Act. Second, since 1954 the CIA has sought special arrangements with the Department of Justice designed to avoid controversies in these kinds of cases by relieving CIA of its responsibility to report to the Department criminal activity where further investigation might, in CIA's judgment, jeopardize clandestine operations.

A. Legislative Initiatives: Abortive Efforts to Enact An Official Secrets Act

Obviously, some of the problems described earlier in the administration of espionage statutes would be resolved if the culpability requirements were eased. It would be immensely easier to prosecute leaks and espionage if all that had to be proven was that the defendant had passed classified information to unauthorized persons -- essentially the rule under the Official Secrets Act.*

According to Professor Benno Schmitt of Columbia Law School, one of the nation's experts on our espionage statutes, proponents

---

* It should be noted that the Official Secrets Act not only applies to divulgence but also to publication of secrets, and that its scope extends to all official government information, not just national security secrets.

of such legislation "reached back to Civil War experience, in which the Union cause had been hindered by newspaper detailing of military plans prior to their execution." The most famous confrontation in the Congress over this kind of legislation was during the Wilson administration when, according to Professor Schmitt, the administration "proposed to censor or make punishable after the fact (exactly which option was never made clear), publication of defense information in violation of Presidential regulations, without any limiting culpability requirement." According to Schmitt:

> In response to this proposal, the Congress engaged in its most extensive debate over freedom of speech in the press since the Alien and Sedition Acts. The preoccupation was not an academic one. Opponents feared that President Wilson or his subordinates would impede, or even suppress, informed criticism of his administration's war effort and foreign policy under the guise of protecting military secrets...The aggrandizing of presidential powers during wartime was a recurrent fear of Republicans, especially Senate progressives such as Borah, LaFollette, Norris and Hiram Johnson.

The proposal was ultimately voted down and only the more modest of the Wilson administration's espionage proposals were adopted. That legislation serves as the framework for our present espionage statutes.

Similar proposals were made during the World War II period. In 1946 the Joint Congressional Committee for Investigation of the attack on Pearl Harbor recommended that Congress enact legislation prohibiting the revelation of any classified information. During the war there had also been a study jointly conducted by Army and Navy Intelligence and the FBI which made

similar recommendations transmitted by the Secretary of War to the Attorney General in June, 1946.

In 1947, the predecessor of Section 798, making it a crime per se to reveal communications intelligence, was introduced and in September of 1948 an omnibus bill was proposed by the Truman administration incorporating the Section 798 language and a number of earlier proposals for simplifying the culpability requirements of the espionage statutes. During this period the CIA, objecting to what it called a "piecemeal" approach of amending various sections of the espionage statutes to deal with special limited problems, suggested a redrafting of the whole espionage statute along the lines of the British Official Secrets Act. A few of the technical changes proposed by the Truman administration, and the intelligence and the military departments were incorporated into Title 18; the most significant of those was Section 798 of Title 18. However, the intelligence community and Department of Defense were not satisfied with those amendments and in 1952 Defense Secretary Robert Lovett proposed to President Truman that the administration still seek legislation similar to the British Official Secrets Act. The Justice Department prepared such legislation but it did not reach the floor in either House.

In 1957 the Commission on Governmental Security suggested legislation that would make it a crime "for any person willfully to disclose without proper authorization for any purpose whatsoever, information classified, knowing such information to have been so classified." The Commission justified its proposal in terms of the "gray mail" problem:

> Since espionage cases may frequently involve national security information of the highest classification, the government is confronted with a serious problem of how far such information can be compromised in the course of prosecution...A defendant who may have met with the greatest success in securing our most precious secrets, may also have secured an advantage in warding off successful prosecution.

No action was taken on the Commission's recommendation, nor on subsequent initiatives in 1958 in the Eisenhower administration, nor a similar initiative in 1966 by the CIA. Indeed, legislation was never seriously considered in this area until the Federal Criminal Code Reform legislation was introduced by the Nixon administration. That legislation contained some of the recommendations suggested by the intelligence community in the past but met with strenuous opposition from media and civil liberties groups. Similarly, those same groups strongly criticized legislation drafted by the CIA and proposed by the Ford administration in February of 1976. No action has been taken on the CIA proposal.

Typical of the type of opposition that the Federal Criminal Code Reform and the subsequent Ford administration proposal provoked is the testimony of Jack Landau of the Reporters Committee for Freedom of the Press before a Congressional subcommittee which was considering the Federal Criminal Code Reform:

> It is abundantly clear that S. 1 (the Code reform proposal) is an unwise and unconstitutional proposal which could be used to silence the type of aggressive news reporting which produced articles about the Pentagon Papers, the Mylai massacre, the Watergate cover-up, the CIA domestic spying, the FBI domestic spying and other government misdeeds: News reporting which has been embarrassing to some persons in the government and which is dependent in whole or

> in part on government compiled information and reports frequently supplied to the press by present or former government employees without government authorization.

The new espionage provisions of the Federal Criminal Code Reform were dropped prior to its consideration by the Senate early this year; proponents realized that any further action on the Federal Criminal Code Reform would be indefinitely postponed as long as there was significant controversy over its constitutionality.

B. Administrative Initiatives

In February of 1954 Lawrence Houston, General Counsel for the CIA, established an arrangement with William Rogers, Deputy Attorney General, to obviate the need to report to the Department of Justice certain criminal activity coming to CIA's attention. According to a memorandum by Houston to Admiral Turner, Houston justified this arrangement to Rogers in the following terms:

> Occasionally, however, the apparent criminal activities are involved in highly classified and complex covert operations. Under these circumstances, investigation by an outside agency would not hope for success without revealing to that agency the full scope of the covert operation involved as well as this agency's authorities and manner of handling the operation.

Apparently, Rogers agreed with this assessment and "saw no purpose in referring the matter to the Department of Justice" under the circumstances. There is some uncertainty in the materials the Committee has reviewed as to whether this arrangement was ever to have been reduced to writing or any formal understanding between CIA and the Department of Justice.

The ambiguity of the arrangement is highlighted by an exchange of correspondence between the CIA and the Bureau of the

Budget in August of 1954. The CIA expressed concern regarding legislation about to be enacted which would grant the Attorney General exclusive responsibility for investigating all violations of Title 18 by government officers and employees. Notwithstanding the CIA's concerns, that legislation was eventually enacted and codified as 5 U.S.C. S.311(a) (since recodified in 28 U.S.C. S.535(b)(2), see Appendix).

In November of 1958, Rogers sent a memorandum to the heads of all departments and agencies in the Executive branch of government emphasizing their responsibilities under the legislation. Subsequent Attorneys General have issued the same reminder soon after taking office. However, for over twenty years the CIA, based on its 1954 arrangement, assumed these directives exempted reporting the kinds of cases Houston had described to Rogers. Although there were minor changes in the procedures described in Houston's original memorandum -- in 1955 and again in 1964 -- the basic thrust of the arrangement wherein CIA took primary responsibility for balancing the need for secrecy against the administration of justice remained until 1975.

Dec. 74

In ~~January of 1975~~ DCI William Colby and Lawrence Silberman, Acting Attorney General, reviewed the 1954 arrangement. At that time Silberman took the position that the agency should comply with 5 U.S.C. S.311(a) by providing a summary "but not an investigative report as such" in essentially every case and that the basic security issue should be raised, but that the Attorney General, not the CIA, would make the decision on whether or not to prosecute. The responsibility of the CIA to report evidence

P76 House God Ops Hearings

of crimes by its employees to the Attorney General was the subject of a specific provision in Executive Order 11905 issued by President Ford (designed to regulate the activities of the intelligence community) and its successor issued by President Carter, Executive Order 12036.

The Attorney General and DCI are currently attempting to develop a memorandum of understanding which would serve as a successor to the 1954 arrangement. The new Executive Order and the draft memorandum of understanding between Justice and CIA retain the principle established by acting Attorney General Silberman that the Department of Justice has the responsibility of balancing the needs of secrecy against the ends of justice.

Both the memorandum of understanding and the Executive Order purport to impose a burden on the intelligence community to report criminal acts by its own employees. With respect to non-employees, the new Executive Order reads as follows:

> ...(the head of any intelligence agency must) report to the Attorney General evidence of possible violations by any other person of those federal criminal laws specified in guidelines adopted by the Attorney General.

No such guidelines have yet been adopted and, therefore, the reporting requirements under that provision are unclear. Furthermore, neither the memorandum of understanding nor the Executive Order address the way in which the Department of Justice should handle evidence necessary to investigate or prosecute an allegation brought to its attention under these provisions. In other words,neither the memorandum of understanding nor the Executive Order are intended to resolve the controversies on the use of classified information in the

prosecution or investigation of crimes, the problem to which this report is addressed.

Certainly one of the difficulties in developing these policies is concern that these reporting requirements might indirectly involve the foreign intelligence agencies in domestic law enforcement in violation of the 1947 National Security Act. The Committee shares this concern. However, the solution to this dilemma may be in the distinction between passively reporting domestic criminal activity on the one hand and actively seeking it out (e.g., "watchlisting" domestic subversives). The drafters of the memorandum of understanding and regulations implementing the Executive Order should keep this distinction in mind and avoid an unrealistic interpretation of the domestic law enforcement prohibition.

VII. NEW INITIATIVES

The Committee agrees with former DCI Colby's testimony before the Subcommittee on Secrecy and Disclosure that, "We would be irresponsible if our revision of intelligence structure did not recognize the need to protect the necessary secrets of intelligence better than we do today." A resolution of the dilemma presented by this report must be a part of the charter legislation being considered by the Intelligence Committee.

To meet the problems set out in this report, the Committee has prepared a recommended program.* This program is designed to serve two basic ends: first, to facilitate the enforcement of espionage statutes and thereby protect our national secrets without jeopardizing constitutional principles; and second, to facilitate enforcement of the criminal sanctions set out in the legislative charters. Without question, the movement to apply the rule of law to intelligence through statutory charters will be severely undermined if leakers or spies continue to go unpunished or if violations of the charters go unenforced.

A. Leaks and Espionage Generally

The classical espionage statutes cover situations where a person knowingly gives national security information to an agent of a foreign power. (Prosecution of a spy under these statutes often fails in the face of the "gray mail" phenomenon.) In addition, although disclosure of communications intelligence

ILLEGIB — CIA to support this non- The one in the Leak cases have failed — lot of them

* The Committee's recommended program is contained in seven recommendations found in Part VIII, infra.

and atomic energy secrets is clearly punishable under current law, most leaks are not, because of the lack of criminal intent or direct communication to a foreign agent. The leaker's intent is not ordinarily criminal, because he customarily leaks to a newspaper, not a foreign agent. In fact, the leaking of national security information has become an informal and quasi-legal system. For example, senior officials often disclose classified information as a means of explaining their positions to the public, while dissenters leak in order to expose improprieties and shoddy thinking. There are two major drawbacks to the sub rosa practice of providing selected intelligence information to the news media and other sources. First, the public does not necessarily receive a balanced view from the leaked information because the process is informal. Second, and more importantly, information whose secrecy is vital to our national security is sometimes disclosed.

Administrations from the time of World War I have put forward plans to make the disclosure of government secrets a crime even without intent to damage the national security or communication to a foreign agent. Nevertheless, all these attempts have foundered, partly due to the inevitability of faulty classification. Congress has felt it improper to punish someone for releasing information which should not in fact have been restricted. And, as shown above, offering proof in open court that a certain piece of information damaged the United States ensures that the damage will be done by confirming the veracity of the information.

Although the mere classification of a document may not in itself warrant criminal penalties for its disclosure, certain classes of information are in fact so sensitive that a statute should protect them.

Former Director Colby testified in favor of a proposal that would impose such strict liability penalties upon the unauthorized disclosure by government employees of sensitive sources and techniques of intelligence collection. To an extent the Committee anticipated Colby's recommendation in a provision of its proposed legislative charter (S. 2525, Sec. 431(a)). This section penalizes the disclosure of the identity of a CIA employee serving under cover in a manner which jeopardizes the safety of that employee. Colby, however, suggests that the sanction be expanded to cover CIA sources as well as employees and circumstances where political or economic reprisals could be expected. Although Colby urges protection for intelligence "techniques," the Committee is extremely hesitant in going beyond the strict liability coverage already accorded communications intelligence. Colby himself warned the Committee of the great difficulties inherent in developing a workable definition of "technique." Added to the difficulty of legally defining "technique" are the difficulties of proving that any given disclosure revealed it.

As this report clearly establishes, the existing espionage statutes are unenforceable in the face of the "gray mail" phenomenon and any new statutes would face the same problem. Therefore, while the modest expansion of the espionage statutes described in the preceding paragraph may warrant serious

consideration, a major restructuring of those statutes to encompass all leaks is not now warranted.

If leaks cannot then be curtailed by criminal sanctions, what will diminish their frequency and gravity? Any comprehensive law against leaks cannot be effective so long as it is impossible to distinguish between a criminal act and a widely accepted governmental practice. Past Executive Orders on classification have failed to protect the most important national security information by providing for the classification of much information that ought to be made public. Recently, President Carter promulgated a new order dealing with secrecy and classification. The effects of this new Order are not yet apparent, but if it continues to mandate excessive secrecy, the Order will foster disrespect for the whole classification system. In the words of Justice Stewart in the Pentagon Papers case: "When everything is secret, nothing is secret." Perhaps the mechanisms contained in the new executive order will avoid overbroad classification and will allow for declassifying intelligence necessary to informed public debate and thus minimize the incentive behind unauthorized disclosure of information.*

Yet, given the ingrained nature of the leaks system and the fact that leaks often result from bureaucratic infighting, some unauthorized disclosure is bound to continue. To deal with leaks

---

* Of course, such a declassification system must be impartial. Otherwise, the public will be faced with a biased view and officials disagreeing with this view would have added incentive to leak.

administrative sanctions are better suited in most cases than criminal ones because they are more enforceable. No risk of "gray mail" would exist, because proceedings could be secret. Due process rights must, of course, be preserved. At the same time, administrative sanctions would be less onerous. Dismissal or loss of security clearance for leaking often more strictly adheres to the rule of Messrs. Gilbert and Sullivan -- "Let the punishment fit the crime."

B. Facilitating Enforcement of Existing Statutes and the Charters

The review of the cases described earlier and the hearings of the Secrecy and Disclosure Subcommittee have led the Committee to recommend a program of both administrative and legislative action designed to facilitate enforcement of the espionage statutes. In essence, on the administrative side, the Committee recommends a streamlining of decisionmaking within the Executive branch on cases where leaks or espionage occur and to encourage the use of administrative sanctions in less serious breaches of security or other violations of the law. On the legislative side, the Committee recommends a variety of new judicial procedures intended to strengthen the hand of the judge and encourage accommodation between the defendant and the prosecutor concerning the use of classified information in litigation -- to seek solutions which encourage proceeding with prosecution rather than dropping the case out of fear of disclosure of sensitive information.

(1) Administrative Recommendations

At the heart of its administrative recommendations (see pp.) is the Committee's concern that there is no effective administrative system currently operating in the Executive branch for investigating and penalizing unauthorized disclosures and the crimes of bribery, perjury and others described in Part V. Leakers occasionally are penalized on an

ad hoc basis.* Violations of the Executive Order on classification, and even classical espionage, are not subject to formal administrative sanction.

In the case of leak investigations the FBI takes the position that it should not investigate a leak unless there is clear evidence of a crime. The Committee believes that the FBI should not conduct investigations of citizens without their consent except in cases involving a nexus with criminal activity.

However, even where prosecution of the crime is impossible because of the risk of further disclosures, the FBI should investigate if --

1) the leak endangers sensitive intelligence sources or methods and is reasonably believed to violate the criminal statutes of the United States;

(2) the persons investigated are Government officials having access to the information leaked;

(3) the investigation and any intrusive investigative techniques are authorized in writing by the Attorney General;

(4) the investigation terminates within 90 days, unless such authorization is renewed; and

(5) the Attorney General submits information concerning the leak to the head of the employing agency, or to the President, for appropriate administrative action.

---

* E.g., Donald Stewart, formerly the chief leak investigator for the Department of Defense, supplied examples of cases during his tenure when high-ranking military officials received a "slap on the wrist" for what appeared to be serious compromises. Mr. Stewart's prepared statement appears as part of the Subcommittee's public hearing record.

These standards do not go as far as the recommendations of the Rockefeller Commission (on alleged CIA abuses), which proposed FBI investigations without evidence of a crime or the Attorney General's approval. Nevertheless, they break sharply with current Justice Department policy foreclosing FBI investigations of damaging criminal leaks where administrative action, rather than prosecution, is the intended result.

The Justice Department is properly concerned that such cases waste time and money because they often turn out to be leaks either formally or informally sanctioned by appropriate authorities. Nevertheless, where such a leak endangers sensitive sources or methods and violates the criminal statutes investigation is appropriate. The higher the criminal leaker, the more important it is to bring in the FBI and the Attorney General, regardless of the inability to prosecute.

The Director of Central Intelligence has extraordinary powers under the 1947 National Security Act, and will have similar authority under the new legislative charters, to dismiss CIA employees. With that authority comes the implied responsibility to investigate employees' past activities which would warrant dismissal. This investigative authority should not be delegated to the FBI except in the case of explicit criminal violations. Some organization with intelligence community-wide authority should be required to investigate activity by intelligence agents, employees or informants which violates security or charter prohibitions.

As stated, the advantage of administrative sanctions over criminal prosecution is that procedures under the former do not

require extensive public disclosure of classified information. Therefore, both the staff of the Committee and representatives of the Executive branch should explore what possibilities exist for formalizing and upgrading administrative review and investigation procedures for violations of security and other unlawful acts by intelligence officials. For example, a possible alternative is an administrative review procedure for employees similar to courts martial in the military. Officials of the agency would hear complaints of violations, especially in circumstances where the decision has been made to forego criminal proceedings for national security reasons. These administrative review procedures could be applied to former employees who violate charter prohibitions, assuming that a deferred compensation pension plan has been conditioned upon continued compliance with security and charter requirements. Former employees who violate prohibitions could be subject to loss of pension rights through the administrative procedure, although this procedure would raise constitutional "due process" issues. more as hell would

Another major goal of the Committee recommendations for administrative action is to improve accountability in Executive branch decisionmaking concerning cases involving national secrets. The Committee agrees with the testimony of [redacted] STAT before the Secrecy and Disclosure Subcommittee:

STAT [redacted]

> I have the sense that the government may be aborting cases prematurely or unecessarily because of a failure to press the alternatives to their fullest, as we did, for example, in the Special Prosecutor's Office in the Ellsberg break-in prosecution, where defense efforts to use "national security threats" to stymie the case were beaten in the courts.

if classes are frivolous - they are no problem

During the course of the hearings the Subcommittee members and witnesses agreed on a number of fundamental points about decisionmaking in these cases. There is little controversy that the ultimate decision on whether to proceed on these types of cases must be centralized within the Attorney General's office. The DCI should have shared authority with the Attorney General through the "sources and methods" provision of the National Security Act to halt prosecution investigation of a criminal case. The Deputy Attorney General and the DCI in testimony before the Subcommittee agreed that it was up to the Attorney General, with disputes settled by the President, to decide whether or not the jeopardy to national secrets in pursuit of an investigation outweighs the ends of justice.

Back to 54 agreement - we don't want this

If the intelligence community disagrees with an Attorney General's decision, the DCI may appeal to the President. The decision to drop a national security case should be made in writing by a high-level official within the Department of Justice, an Assistant Attorney General or a Deputy Assistant Attorney General. Included in that written decision should be a detailed explanation of the information which would have been revealed in the course of trial, why the information would be revealed, and what damage the disclosure of the information would have to the national security. The mere fact that a written record must be made will discourage thoughtlessly dropping a potential prosecution.

A final area appropriate for administrative action pertains to the requirement that intelligence agencies report to the Department of Justice evidence of criminal activity by employees.

As noted in Part VI of this report, the administration is currently at work attempting to implement provisions of the new Executive Order and to update the so-called Silberman-Colby understanding as to the requirements of the intelligence community to report crimes of its employees to the Department of Justice. If there is no mechanism through which the Department of Justice is so notified, the law enforcement process is likely to break down.

Thus the so-called Silberman-Colby understanding should be updated and formalized. It is equally important that the memorandum of understanding be expanded in scope to address not only criminal activities of intelligence agents, employees or assets, but also criminal activity known by the intelligence community which does not involve its employees or assets. Such an understanding must consider the protection of sources or methods.

(2) Legislative Initiatives

The purpose of the legislative suggestions set out in Part VIII is to provide alternatives which will allow prosecutors to avoid what one witness described as the "disclose or dismiss dilemma." Because of ambiguities in existing judicial procedures or because of a general reluctance on the part of the intelligence community and the Department of Justice to take the chance of pursuing these cases, the administration must decide whether to disclose intelligence information or to dismiss a criminal case or not pursue an investigation at the outset.

However, the dilemma posed by the introduction of sensitive intelligence information into criminal cases, especially at the behest of the defendant, can frequently be avoided because the information is requested for an irrelevant matter. For example, Lacovara described to the Subcommittee the following sequence in the prosecution of the Watergate burglars for the break-in of Dr. Ellsberg's psychiatrist:

> After the indictment was returned, the defendants did in fact demand the production of highly classified files, including nuclear missile targeting plans. The defendants were seeking to utilize discovery to obtain national security information in order to support the purported defense that they believed the break-in was justified by national security concerns. The special prosecutor argued, however, and both District Judge Gesell and the U.S. Court of Appeals for the District of Columbia Circuit agreed, that the information sought was irrelevant because "good faith" motivation was not a valid defense against the crime charged, conspiracy to violate Fourth Amendment rights. Thus the difficulty of choosing between forfeiting an important criminal prosecution or disclosing information potentially damaging to our national security was avoided.

In many other cases it is clear that if the prosecutor had forced the court to carefully examine the relevancy of the intelligence information to a purported defense or motion, the judge may well have been forced even under the present standards of relevancy to decline the request for the information. However, administration witnesses were reluctant to rely on the relevancy standard. They argued that what one judge found relevant another judge would find irrelevant and that many judges grant the discovery motion first before deciding whether or not the intelligence information will be used in the case. Furthermore, defense counsel routinely make sequential discovery motions which harrass the prosecution and thus tie up the

prosecutors in negotiations with the CIA over sensitive documents.

STAT [redacted] suggests that Congress enact an omnibus pre-trial proceeding for use in all cases where classified exhibits or testimony would be required. The defendant would be required to put the prosecutor and the court on notice in advance of trial of all motions he would make requiring discovery of sensitive classified intelligence information when he might have reasonably known of the need for discovery prior to trial. He would have to argue successfully the relevancy of each motion before the court in order to secure discovery of the documents or testimony. For the purposes of argument, the court could assume that the documents existed without actually providing the defendant the documents and could decide in advance whether the defense would be permitted or the motion granted as a matter of law. This process would be intended to "weed out" irrelevant defenses and thus simplify prosecution of the case. If at some later time a new matter arose requiring a special motion or defense which in turn required the disclosure of secrets, the court could still entertain an appropriate discovery motion and both the government and the defendant would be entitled to an interlocutory appeal.

If such a special omnibus procedure is adopted, the Committee recognizes that there will be cases where the "weeding out" process will actually arrive at motions and defense arguments that do require the use of intelligence information. At that point the judge must decide two basic questions: (1) Is the information in question truly national security information, the disclosure of which would damage the national security? (2)

What action should he take against the prosecution if it withholds the documents or testimony (e.g., dismissal of the case)? Of course, the Government always has the option of dismissing a prosecution if the court's decision on these matters would require what it believes to be excessive disclosure.*

In 1974 the Supreme Court proposed an amendment to the Federal Rules of Criminal Procedure known as the Federal Rules of Evidence. These Rules of Evidence were extremely controversial in the Congress because they contained a provision, Section 509, that defined a "secret of state" privilege. An invocation of the privilege by the government would prompt an in camera adversary proceeding in which the parties would litigate whether the information in question was in fact "a secret of state".

Section 509 was rejected by the Congress as it reviewed the rules proposed by the Supreme Court. However, several witnesses agreed that perhaps Section 509 might serve as the basis for an in camera adversary proceeding that would resolve the use of intelligence information in the course of a trial after the "weeding out" process described above. Furthermore, several adjustments to the Section might be made to respond to criticism which led to congressional rejection in 1974. For example, the new state secret privilege might more narrowly define the types of information to which the government could invoke the

---

* The Government does not undertake prosecution on a whim. In deciding to drop an indictment the Attorney General must weigh the expenditures of time and money in investigation and prosecution, as well as fairness to the defendant who must live with the stigma of an unchallengeable indictment.

privilege. It might give a greater role to the court in reviewing the claim of privilege, including authority to go beyond and behind the classification to determine the actual damage to the national security if the information were disclosed. It might guarantee the presence of the defendant and his counsel in the in camera procedure, subjecting both to contempt of court and possible espionage prosecution if they disclose the results of the procedure.

The primary purpose of such a procedure would be to set standards to place the prosecution and the government on notice in advance on what types of information could be subject to privilege and to give the judge primary responsibility for administering the privilege. [redacted] in his testimony emphasized the importance of providing judges with some guidance as to what action should be taken if they find the privilege is legitimately invoked. [redacted] suggests a "sliding scale" of sanctions available to the judge so that "the remedy available to the defendant would vary depending upon the circumstances of the case." [redacted] goes on to further describe his proposal as follows:

STAT

STAT

STAT

> At one end of the scale for example, if the defendant's possible use of the information is totally speculative, the case simply would continue without disclosure. At the other end of the scale, where the information is central to the question of guilt or innocence and where no other alternative to public disclosure is possible, dismissal may be necessary. In between, procedures such as instructing the jury to assume that the missing information would have proven a given proposition may be possible. Certainly the Department of Justice should press for some intermediate treatment like that before deciding that the case must be abandoned.

probably could do today still, not much of a problem

VIII. RECOMMENDATIONS

The recommendations which follow were formulated by the Secrecy and Disclosure Subcommittee and are endorsed by the full Committee. They will serve as an agenda for the Committee as it proceeds with consideration of legislative charters. The staff will be developing specific legislative proposals to implement these recommendations for inclusion in the charters to be discussed in the course of its ongoing hearings. It is the Committee's hope that the Executive branch will work with the Committee on these matters and, in particular, on its recommendations for administrative action.

I. The Congress should not at this time consider any general recasting of the federal espionage statutes along the lines of the British Official Secrets Act. Limited further protection of sources and methods, especially human sources, may be required, however. Congressional energies would be better spent on developing procedures to facilitate enforcement of existing statutes.*

II. The Executive branch should interpret the new Executive Order on security classification with an emphasis on decreasing the amount of unnecessary secrecy. The intelligence community, the Intelligence Oversight Board, and the intelligence committees of the Congress should declassify as many as possible of their reports and studies on matters of public concern to discourage the "leaking" of versions which have not been sanitized to protect "sources and methods" information. These reports and studies must be declassified in a disinterested manner, so that the public receives the true view of a given situation.

III. The intelligence community should develop, in conjunction with the Committee, administrative review procedures for the exercise of the DCI's authority for the dismissal of employees for violations of security

---

* For discussion of the Committee's rationale for recommendations I and II, see pps. , supra.

or other provisions of the intelligence community charter. At the same time the intelligence community should centralize authority, perhaps in the Intelligence Oversight Board, for investigations of breaches of security and violations of charter prohibitions which do not constitute crimes. The purpose of these procedures would be to permit sanctions against employees who violate the charter through procedures similar to a military court martial where it is easier to cope with classified documents or testimony than in traditional public criminal trials. Some consideration should also be given to applying these administrative review procedures to former employees through withdrawal of pension rights for former employees who violate security or provisions of the charter.*

IV. The FBI should continue to have exclusive responsibility for investigating criminal violations involving the intelligence community. In leak cases the FBI should initiate investigation if:

(1) the leak endangers sensitive intelligence sources or methods and is reasonably believed to violate the criminal statutes of the United States;

(2) the persons investigated are Government officials having access to the information leaked;

(3) the investigation and any intrusive investigative techniques are authorized in writing by the Attorney General;

(4) the investigation terminates within 90 days, unless such authorization is renewed; and

(5) the Attorney General submits information concerning the leak to the head of the employing agency, or to the President, for appropriate administrative action.

V. The Attorney General should issue regulations that are binding upon all departments of the government which set out the procedures whereby agencies of the intelligence community are to report crimes that come to their attention and to provide necessary information to attorneys of the Department of Justice to proceed with a criminal investigation or prosecution.

---

* For discussion of the Committee's rationale for recommendations III, IV, V, and VI, see pps. , supra.

The regulations should also set out how the decision is to be made not to proceed in national security cases and who is authorized to make such a decision. These regulations should require that any such decision be made in writing and the decision paper should include the precise intelligence information which would have been disclosed in the course of the trial, why the official believes it would have been disclosed, and the damage the information would have to the national security if the case proceeds. The decision paper should be available to the intelligence oversight committees of the Congress and such cases should be reported to the committee annually or as required.

VI. The Executive branch should complete its memorandum of understanding between the Attorney General and the DCI on the responsibility of the intelligence community to report crimes to the Department of Justice. The memorandum of understanding should be expanded to cover reporting of all activity in violation of U.S. laws coming to the attention of the intelligence community, but must consider protection of sensitive sources and methods.

VII. Congress should consider the enactment of a special omnibus pre-trial proceeding to be used in cases where national secrets are likely to arise in the course of a criminal prosecution. The omnibus procedure would require the defendant to put the prosecution and the court on notice of all motions or defenses or arguments he intended to make which would require the discovery and disclosure of intelligence information or the use of intelligence community witnesses. The judge would be required to rule in advance of the trial on the admissibility of the intelligence information and on the scope of witnesses' testimony as well as the general relevancy of the motion or defense prior to granting discovery of any intelligence information to the defendant. On the other hand, the defendant would be permitted a discovery motion during the course of trial if the prosecution presents a matter not originally suggested by indictment or for which the defendant could not fairly have been expected to be on notice at the time of the omnibus procedure.*

---

* For a discussion of the Committee's rationale for recommendations VII and VIII, see pp. f.f., supra.

VIII. The Congress should reconsider the secret of state privilege proposed by the Supreme Court in 1974. That privilege needs to be considerably revised along the lines described above but at a minimum should provide for an in camera adversary procedure on the privilege, define the scope of the privilege, the standards for its invocation, provide increased judicial authority for its procedural administration, and provide a sliding scale of sanctions available to the judge in the case where the privilege is successfully invoked.